AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One Samsung Galaxy with IMEI 352818706769185172, currently in the custody of the DEA Philadelphia Field Division

Case No. 19-1293

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Eastern District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. Sections 841, 846	attempt to possess with intent to distribute controlled substances

The application is based on these facts:

See Attachment C.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Travis W. Campbell, DEA Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: July 26, 2019

Judge's signature

City and state: Philadelphia, Pennsylvania

Hon. Carol S. Wells, U.S. Magistrate Judge
Printed name and title

ATTACHMENT C

AFFIDAVIT

I, Travis W. Campbell, being duly sworn, depose and say:

1. I am a Special Agent with the Drug Enforcement Administration ("DEA") and have been so employed since April 2015. In October 2015, I was assigned to the DEA Philadelphia Field Division. Prior to my employment with the DEA, I was a Special Agent with the North Carolina State Bureau of Investigation/Alcohol Law Enforcement for approximately 5 years.

2. I have specialized training and experience in drug smuggling and distribution investigations, including but not limited to, the means and methods used by traffickers to import and distribute controlled substances, interdiction, smuggling methods, and the concealment and laundering of proceeds from illegal drug trafficking activities. I have participated in numerous narcotics investigations, debriefed or participated in debriefings of hundreds of defendants, informants, and witnesses who had personal knowledge regarding major narcotics trafficking organizations, and have participated in all aspects of drug investigations, including conducting physical surveillance, analyzing information obtained from court-ordered pen register and trap and trace intercepts, and analyzing telephone toll information. I have been the affiant in numerous wiretap investigations and also assisted in monitoring the wiretap communications. My training and experience have made me familiar with illegal drug trafficking and the packaging and shipping of controlled substances including heroin, cocaine, cocaine base ("crack"), methamphetamine, and marijuana. I am aware that drug traffickers commonly use cellular telephones in furtherance of their drug trafficking activities and frequently change

cellular telephone numbers and cellular telephones in an effort to thwart law enforcement's use of electronic surveillance. I am also aware that drug traffickers often speak in vague, guarded, or coded language when discussing their illegal business in an effort to prevent detection. My narcotics training and experience have made me familiar with the methods of illegal trafficking, packaging and shipping of the following controlled substances: methamphetamine, cocaine, cocaine base, heroin, and marijuana.

3. Based on my training and experience, I know that those involved with drug trafficking commonly utilize their cellular telephones to communicate with co-conspirators to facilitate, plan, and execute their drug transactions. For example, I know that drug traffickers often store contacts lists, address books, calendars, photographs, videos, and audio files, text messages, call logs, and voice mails in their electronic devices, such as cellular telephones, to be used in furtherance of their drug trafficking activities.

4. Specifically, I know that those involved in drug trafficking communicate with associates using cellular telephones to make telephone calls. If they are unable to reach the party called, they frequently leave voice mail messages. I am aware that Apple-based and Android-based phones download voice mail messages and store them on the phone itself so that there is no need for the user to call in to a number at a remote location and listen to the message. In addition, I know those involved in drug trafficking communicate with associates using cellular telephones and tablets to send e-mails and text messages. I know they also communicate with associates via social media networking sites and through messaging options via social media (e.g., Facebook messaging), or through other communication applications available to download and use on phones, including but not limited to "Whatsapp," "Tango," and "Hangouts." By

analyzing call and text/application communications, including any social media "chats" or messaging application communications, I may be able to determine the identity of co-conspirators and associated telephone numbers, as well as if there were communications between associates during the commission of the crimes.

5. Furthermore, cellular telephones also contain address books with names, addresses, photographs, and phone numbers of a person's regular contacts. I am aware that those involved with drug trafficking frequently list co-conspirators in directories, often by nickname, to avoid detection by others. Such directories as the ones likely contained in the seized cellular telephones, are one of the few ways to verify the numbers (*i.e.*, telephones, pagers, etc.) being used by specific co-conspirators.

6. In addition, I know that those involved with drug trafficking often take photographs or make videos of themselves and their co-conspirators and retain them on their electronic devices such as cellular telephones. This evidence would show associations between accomplices, *i.e.* photographs of accomplices and/or individuals common to co-conspirators. I am also aware that drug traffickers often take photographs or make videos of drugs and drug proceeds with their cellular telephones and tablets. Based on my training and experience, those who commit these crimes often store these items on their phones in order to show to associates, and/or to upload to social media.

7. Based on my training and experience and the training and experience of other agents, I am aware that data stored on electronic devices can remain for a long time. Furthermore, I am also aware that newer phones can store and contain data from several years ago, for instance if an individual uses a social media or messaging application, that stores data

from several years ago (such as Facebook messenger, Whatsapp, Tango). In addition, I am aware that some data, such as contacts, photographs, and text messages, can be transferred from old phones to new phones, either manually or by transferring a SIM card device that has the data on it. It is therefore reasonable to believe that the phones recovered from Virginia BASORA Gonzalez, Reynaldo ORTEGA Basora may have data stored from their interactions with co-conspirators during the course of the charged conspiracy, or may have older communications from social media sites stored on the phone.

8. Furthermore, based on my training and experience and the training and experience of other agents, I know that drug traffickers often use a cellular phone's Internet browser for web browsing activity related to their drug trafficking activities. Specifically, those involved with drug trafficking may use an Internet search engine to explore where banks or mail delivery services are located, or may use the Internet to make reservations for drug-related travel. In addition, I know that drug traffickers also use their cellular telephone's Internet browser to update their social networking sites in order to communicate with co-conspirators, and to display drugs and drug proceeds or to post photographs of locations where they have traveled in furtherance of their criminal activities.

9. In addition, drug traffickers sometimes use cellular telephones as navigation devices, obtaining maps and directions to various locations in furtherance of their criminal activities. These electronic devices may also contain GPS navigation capabilities and related stored information that could identify where these devices were located.

10. Furthermore, based on my training and experience, forensic evidence recovered from the review of a cellular telephone can also assist in establishing the identity of the user of

the device, how the device was used, the purpose of its use, and when it was used. In particular, I am aware that cellular telephones are all identifiable by unique numbers on each phone, including: serial numbers, international mobile equipment identification numbers (IMEI) and/or electronic serial numbers (ESN). The search of each phone helps determine the telephone number assigned to each device, thus facilitating the identification of the phone as being used by members of the conspiracy. In addition, I am aware that by using forensic tools, information/data that users have deleted may still be able to be recovered from the device.

11. I make this affidavit in support of an application for a search warrant of: one Samsung cellular phone with IMEI 352818706769185172 (SUBJECT PHONE 1). This application seeks authority to search for and seize evidence, and fruit and instrumentalities of crimes against the United States, specifically in violation of Title 21, United States Code, Sections 846(a)(1), as described in Attachment B.

ELECTRONIC DEVICES

12. As described in Attachment B, this application seeks permission to search and seize things that the above items might contain, in whatever form they are stored. As used herein, the term "electronic device" includes any electronic system or device capable of storing or processing data in digital form, in this case referring specifically to wireless or cellular telephones.

13. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices. In particular, I know that electronic devices, including cellular telephones used by drug traffickers, are likely to be

repositories of evidence of crimes. I know that an electronic device such as a cellular telephone may contain data that is evidence of how the electronic device was used, data that was sent and received, and other records that may indicate the nature of the offense.

14. Furthermore, I know that electronic devices, such as cellular telephones, can store information for long periods of time. Examples of such information include, text and multimedia message conversations, call history, voice mail messages, e-mails, photographs, and other data stored on the device. Similarly, I know from my training and experience that when cellular telephones are used to access the internet, a browser history is also frequently stored for some period of time on the electronic device. This information can sometimes be recovered with forensic tools.

15. Based on my experience and training, as well as the experience and training of other agents, I know that even when a user deletes information from a device, it can sometimes be recovered with forensics tools. Further, based on my experience and training, I know that other than the conventional mechanical hard drives that are traditionally in computers, becoming more prevalent are flash memory-based hard drives and devices. This technology has been traditionally used for small thumb drives where files and data are stored electronically, but has since evolved and is being used in computer hard drives known as "solid state hard drives" or SSD's and also being used in cell phones and smart phones. These devices do not operate like mechanical hard drives when it comes to how files and data are stored and deleted. These devices can move data around on the drive to maximize storage space and longevity of the drive, compress data, and may use different deletion techniques for how a deleted file is handled and

overwritten. The manner in which these devices function may limit how much data, if any, can be recovered from these types of devices.

16. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that searching electronic devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of electronic devices and software programs in use today that specialized equipment is sometimes necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of electronic devices, operating systems, or software applications that are being searched.

17. Furthermore, I am aware that electronic data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching electronic devices can require the use of precise, scientific procedures that are designed to maintain the integrity of electronic data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on electronic devices.

18. Also, I know from my training and experience that the volume of data stored on many electronic devices will typically be so large that it will often require a search of the device in a law enforcement laboratory or similar facility. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might

contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

19. I am also aware that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, *i.e.,* space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

20. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), electronic devices can contain other forms of electronic evidence as well. In particular, records of how an electronic device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the electronic devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the electronic device was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time

21. Further, evidence of how an electronic device has been used, what it has been used for, and who has used it, may be the absence of particular data on an electronic device. For

example, to rebut a claim that the owner of an electronic device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the electronic device remotely is not present on the electronic device. Evidence of the absence of particular data on an electronic device is not segregable from the electronic device. Analysis of the electronic device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

22. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time consuming manual search through unrelated materials that may be co-mingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the DEA intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

23. Given that the affidavit is in support of a search warrant for electronic devices, which are stored as evidence with the DEA, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

FACTS ESTABLISHING PROBABLE CAUSE

24. On or about June 3, 2019, DEA Special Agents in the Philadelphia Field Division Group 32, received an investigative lead from the DEA Yuma Residence Office ("YRO") regarding approximately 1,000 suspected fentanyl pills that a source of supply had tasked a DEA undercover agent ("UC") with packaging and shipping to "Maria Ortega" at 108 W Wishart Street, Philadelphia, PA. The YRO investigative agents informed your affiant that the UC was provided the approximately 1,000 suspected fentanyl pills on June 3, 2019 in Arizona by an unknown courier who was acting on behalf of FNU LNU, a/k/a "PELON." After receiving the fentanyl pills from the courier, the UC exchanged messages with PELON via WhatsApp, who requested the UC to send the pills from "Lourdes Ortega" 1240 E California Street, San Luis, AZ 85349 to "Maria Ortega" at 108 W Wishart Street, Philadelphia, PA, 19133.

25. YRO agents conducted a field test of the approximately 1,000 suspected fentanyl pills and received a positive result that the pills contained fentanyl. The pills weighed approximately 244 grams, including the tape they are wrapped in. YRO agents prepared a USPS Medium Flat Rate box with the aforementioned address information provided by PELON and received a USPS Priority 2-Day Postage Paid label with tracking number 9505511459749155362958. The UC agent then sent PELON a photograph of the USPS priority box and the label affixed to the box representing the package as the package that contained the fentanyl pills. YRO agents coordinated with a USPS to show the USPS package was sent to 108

W Wishart Street, Philadelphia, PA, although YRO agents did not actually send the box via USPS. The tracking information for the package shows the package is scheduled for delivery on June 6, 2019 should PELON, or another member of the drug trafficking organization ("DTO"), attempt to electronically track the package.

26. On June 5, 2019, the Honorable Timothy R. Rice, Magistrate Judge for the Eastern District of Pennsylvania, signed a court order authorizing a GPS tracking device and an entry detection device to be installed inside the USPS parcel and an anticipatory search and seizure warrant for 108 W Wishart Street, Philadelphia, PA should the parcel be opened in that location.

27. On June 6, 2019, investigative agents placed two brick-shaped items resembling the original packaging that contained the 1,000 suspected fentanyl pills and installed a GPS tracking device inside one of the sham brick-shaped items. The brick-shaped items were also sprayed with theft detection powder that is detectable under the use of an ultraviolet light.

28. At approximately 11:00 a.m., investigative agents established surveillance at 108 W Wishart Street, Philadelphia, PA. At approximately 11:25 a.m., a USPS Postal Inspector, acting in an undercover capacity, delivered the USPS parcel to 108 W Wishart Street, Philadelphia, PA by placing the parcel on the front door steps.

29. At approximately 11:50 p.m., investigative agents observed a Hispanic male, later identified as Julio Cesar CONCEPCION, arrive outside 108 W Wishart Street, Philadelphia, PA and carry the USPS parcel inside the residence. As agents observed CONCEPCION carry the package inside the residence, the entry detection device emitted an audible sound indicating the package was being moved. The entry detection device then began emitting a different audible

signal indicating the package had stopped moving, but was still unopened. The entry detection device emitted this same signal until Virginia BASORA Gonzalez ("BASORA") entered the location, as described below.

30. At approximately 12:15 p.m., investigative agents observed a Hispanic male, later identified as Reynaldo ORTEGA Basora ("ORTEGA"), exit 108 W Wishart Street, Philadelphia, PA and walk to the corner of N Front Street and W Wishart Street. Investigative agents later observed ORTEGA return to the residence and reenter that location.

31. At approximately 2:30 p.m., investigative agents observed a Hispanic female, later identified as BASORA, exit the passenger-side of a blue Chevrolet Cruz and enter 108 W Wishart Street. After BASORA entered the residence, the entry detection device emitted several audible signals indicating the package was being moved around.

32. At approximately 3:00 p.m., the entry detection device emitted a signal indicating that the USPS parcel had been opened. Investigative agents approached the front door of the residence. Investigative agents knocked several times on the front door and no one answered. Investigative agents then observed ORTEGA climbing the fence in the alleyway behind the 100 block of W Wishart Street. Investigative agents identified themselves to ORTEGA and ordered him to stop. ORTEGA did not comply with investigative agents' commands and fled from the location. Investigative agents pursued ORTEGA and detained him shortly thereafter. Investigative agents checked ORTEGA's hands for the theft detection powder revealing ORTEGA had the powder on his hands. ORTEGA informed investigative agents that he lived at 108 W Wishart Street, Philadelphia, PA. Investigative agents seized an IPhone from ORTEGA at the time he was arrested.

33. Once investigative agents entered 108 W Wishart Street, Philadelphia, PA, agents found BASORA in the kitchen area on the first floor of the residence. BASORA's hands were checked for the theft detection powder revealing she had the powder on her hands. BASORA informed investigative agents she lived at 108 W Wishart Street, Philadelphia, PA, but claimed that CONCEPCION and ORTEGA did not live there. Investigative agents seized an IPhone 6S contained within a pink case on the living room table. BASORA informed investigative agents that the IPhone 6S belonged to her.

34. Investigative agents were unable to locate CONCEPCION during the initial search of the residence. CONCEPCION was subsequently observed in the rear alleyway of the 100 block of W Wishart Street. CONCEPCION appeared to be talking on his cellular phone when investigative agents observed him. CONCEPCION's hands were checked for the theft detection powder revealing CONCEPCION had the powder on his hands. Investigative agents seized a black Samsung cellular phone (SUBJECT PHONE 1) from CONCEPCION.

35. Agents recovered the USPS parcel that contained the two brick-shaped items, the GPS device, and the sham, on the ground near the backyard of 109 W Lippicott Street, the block immediately south of the 100 block of W Wishart Street, Philadelphia, PA.

36. During a search of the basement of 108 W Wishart Street, investigative agents found and seized various items of drug paraphernalia including a grinder and plastic baggies commonly used to package narcotics for resale. During a search of the rear bedroom on the top floor of the residence, investigative agents found a Dominican Republic Passport issued to CONCEPCION, in addition to money transfer receipts with CONCEPCION's name listed as the sender. Investigative agents also found and seized a clear plastic baggie containing what was

later determined by a DEA laboratory to be approximately 108.8 grams of heroin with trace amounts of fentanyl. Also recovered were several plastic baggies containing cutting agents.

37. On July 2, 2019, the Honorable Marilyn Heffley, Magistrate Judge for the Eastern District of Pennsylvania, signed an order authorizing the search of the IPhone 6S found in possession of BASORA and the IPhone found in possession of ORTEGA.

38. During a search of ORTEGA's cellular phone, investigative agents found numerous WhatsApp messages between ORTEGA and CONCEPCION, who used SUBJECT PHONE 1. The profile picture for CONCEPCION's WhatsApp account was a photograph of himself. The messages included voice messages during which ORTEGA asked CONCEPCION to bring a "photo" so that he (ORTEGA) could provide the "photo" to someone else. Based on your affiant's training and experience, I know that "photo" is a common term used by drug traffickers to refer to a sample of controlled substances. Based on your affiant's training and experience, I know that drug traffickers provide free samples of controlled substances to customers so that customers can check their quality prior to purchasing larger quantities. Your affiant believes that ORTEGA asked CONCEPCION to provide him with a sample of controlled substances that he (ORTEGA) could then distribute to a potential customer who would purchase a larger quantity of controlled substances if he was satisfied with the quality. Based on these communications, your affiant knows that CONCEPCION utilized SUBJECT PHONE 1 in furtherance of drug trafficking.

39. Based on the information, facts, and circumstances stated above, your affiant believes the previously identified SUBJECT PHONE 1 seized by law enforcement will provide

investigators with additional information related to the investigation of a drug trafficking organization operating in Philadelphia and elsewhere in the United States.

CONCLUSION

40. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief, and that this declaration was executed on July 26 2019.

Travis W. Campbell
Special Agent
Drug Enforcement Administration

BY THE COURT:

HONORABLE CAROL S. WELLS
United States Magistrate Judge